



DEFENSE LOGISTICS AGENCY  
HEADQUARTERS  
8725 JOHN J. KINGMAN ROAD  
FORT BELVOIR, VIRGINIA 22060-6221

IN REPLY  
REFER TO DG

JUN 07 2007

MEMORANDUM FOR DLA CORPORATE BOARD AND SPECIAL STAFF  
COMMANDERS, DLA FIELD ACTIVITIES

SUBJECT: Policies and Procedures When Personal Information is Lost, Stolen, or  
Compromised

It is Department of Defense (DOD) policy<sup>1</sup>, that the privacy of an individual is a personal right that shall be respected and protected. DOD's need to collect, maintain, use or disseminate personal information about individuals shall be balanced against the right of the individual to be protected against unwarranted invasions of their privacy. Accordingly, all DOD personnel, to include contractors, have an affirmative responsibility to protect an individual's privacy when collecting, maintaining, using or disseminating personal information about an individual.

"Personal Information" means information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. Such information is also known as "personally identifiable information" (PII).

Further, whenever a DOD Component (e.g., DLA) becomes aware that records containing PII are lost, stolen or compromised (i.e., breach)<sup>2</sup>, the potential exists that the records may be used for unlawful purposes such as identity theft, fraud, stalking, etc. The personal impact on the affected individual(s) may be severe if the records are misused. To assist the individual, DOD policy requires that the Component promptly notify the individual of any loss, theft or compromise.

The notification shall be made whenever a breach or suspected breach occurs that involves PII pertaining to the following categories of individuals: a service member, civilian employee, military retiree, family member, DOD contractor, other persons affiliated with the DOD Component (e.g., volunteer) and any other member of the public on whom personal information is maintained by the component. The notification shall be made as soon as possible,

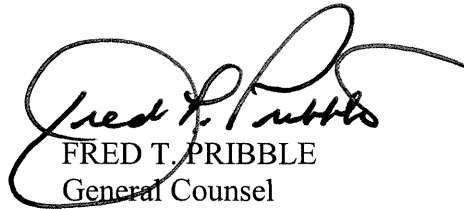
<sup>1</sup> 32 CFR Part 310, "Department of Defense Privacy Program," 72 FR 18758, 13 April 2007.

<sup>2</sup> "Lost, stolen, or compromised information" is defined as actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. Such incidents are also known as "breaches." 32 CFR section 310.4(j)



but not later than ten days after the breach is discovered. A breach or suspected breach shall also be reported to DLA Network Operations Support Center (NOSC) at 1-877-DLA-NEMO within one hour of discovery for immediate forward to the US CERT at the Department of Homeland Security per OMB M-06-19, to the DLA Headquarters Privacy Act Officer within 24 hours, and to the DOD Privacy Office within 48 hours.

In order to meet all of the foregoing DOD policy requirements, attached is a detailed listing of the actions that must be taken by DLA personnel and contractors and concomitant assigned responsibilities.



FRED T. PRIBBLE  
General Counsel

Attachment

## **POLICIES AND PROCEDURES WHEN PERSONAL INFORMATION<sup>1</sup> IS LOST, STOLEN, OR COMPROMISED**

1. The DLA Employee, Service member, or contractor who discovers the breach<sup>2</sup> of personally identifiable information (PII) will immediately call the DLA Network Operations Support Center (NOSC) at:

1-877-DLA-NEMO (352-6366)

2. The NOSC Desk Officer receiving the call will immediately contact the DLA Computer Emergency Response Team (CERT) Watch Officer and the affected local Information Assurance Officer (IAO) if the PII is electronic, or the local Privacy Act Officer (PrivO) if the PII is physical. The DLA CERT Watch Officer will assign an incident tracking number and provide it to the NOSC Desk Officer, who in turn, will relay that number to either the IAO or PrivO.
  - a. If the PII is physical and there is no PrivO at the affected Field Activity, then the NOSC Desk Officer will contact the local Security Officer.
3. If the PII is electronic, the local IAO will notify the local PrivO, and ensure the underlying incident that led to the breach of PII has been contained in accordance with established DOD and DLA Information Assurance policies and procedures.<sup>3</sup> The IAO will continue to report in accordance with established DLA procedures the underlying incident that led to the breach of PII (e.g., computer incident, theft, loss of material, etc.) until the situation has been resolved.
  - a. If containment of the underlying incident requires disabling or disconnecting an information system, the local IAO will contact the DLA Chief Information Officer (CIO) to obtain her approval before proceeding. The CIO may, as deemed necessary, consult with the local Commander and Information Owner prior to her decision to disable or disconnect an information system.
  - b. After obtaining the CIO's decision, the local IAO will affect the decision and then notify the local Commander, Information Owner, and Field Counsel's Office of the CIO's decision.
4. If the PII is physical, the PrivO (or Security Officer, per 2.a. above) will ensure the underlying incident that led to the breach of PII has been contained via investigation, inquiry, or other actions taken to mitigate any harm that could result from such incident in accordance with DOD Privacy Program, 32 CFR Part 310.
5. The DLA CERT will escalate report of the PII incident within one hour via Network Operations (NETOPS) Command and Control Chain to DLA J6 and US-CERT (with a

---

<sup>1</sup> "Personal Information" means information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. Such information is also known as "personally identifiable information (PII)".

<sup>2</sup> Breach is defined as an actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected.

<sup>3</sup> Including CJCSM 6510.01 CH 3 8 March 2006, DLA's Information Assurance Operational Controls One Book chapter, and DLA's Computer Incident Response Plan.

courtesy copy provided to Joint Task Force-Global Network Operations (JTF-GNO))

6. For all PII incidents, the local PrivO will notify both the local Counsel's Office and the local DLA Office of Investigations Field Officer of the incident.
7. For all PII incidents, within the first 24 hours of discovery of the breach, the local Counsel's Office will provide the DLA HQ Privacy Act Officer<sup>4</sup> with details of the incident including the assigned DLA CERT incident tracking number.
8. Within the first 24 hours of discovery of the breach, a local PII Incident Response Team (IRT) made up of the IAO, PrivO, local General Counsel, and DLA Office of Investigations Field Officer must meet and determine whether the PII meets the criteria for being "high impact"<sup>5</sup> PII.
  - a. If the PII is "high impact," then the local Counsel's Office will notify the DLA General Counsel, and copy the DLA Chief Privacy Officer, of this determination no later than 24 hours from the discovery of the breach of PII. The General Counsel's Office will immediately notify the Director, DLA, via the Vice Director, and the CIO's Office, via the Director, Information Assurance, of the "high impact" incident.
  - b. For "high impact" PII incidents, an investigation that follows standard DLA Office of Investigation / AR 15-6 procedures must be performed.
9. If the PII does not meet the criteria for being "high impact" then,
  - a. By the end of the first 24 hours after the discovery of the breach, the local Counsel's office will forward to DLA HQ Privacy Act Officer an incident report containing the following information:
    - i. The date of the breach and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.
    - ii. A brief description of the facts and circumstances surrounding the breach.
    - iii. A brief description of the actions taken in response to the breach, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the breach; whether the affected individuals are being, or will be, notified, if then known, and if this will not be accomplished within 10

---

<sup>4</sup> Contact information for the DLA HQ Privacy Act Officer and DLA Chief Privacy Officer may be found at [http://www.dla.mil/public\\_info/efoia/PrivacyPOC1.html](http://www.dla.mil/public_info/efoia/PrivacyPOC1.html)

<sup>5</sup> High Impact.

- (1) Any Defense-wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act.
- (2) Any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures.
- (3) Individually identifiable medical information.
- (4) Financial information (including SSN).
- (5) Law enforcement and other investigative reports.

*Examples:* A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII. An e-mail containing a scanned note from a physician regarding an employee's medical condition is High Impact PII.

working days, that action will be initiated to notify the Deputy Secretary; what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued; and any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

- b. Within 5 business days of discovering the breach of PII, the PII IRT will make a determination of whether it will be possible for the local Field Activity to provide the required notice to all affected individuals within the mandated 10 business days of discovering the breach of PII.
  - c. If the PII IRT determines that it will not be possible to provide notification to the affected individuals within 10 business days, the local Counsel's Office will prepare a memorandum for the Deputy Secretary of Defense for signature by the Director of DLA providing a brief summary of what occurred, why notification was not provided within the required 10 business days, and what actions being taken, highlighting the exact date notifications will commence and their anticipated completion date.
    - i. This "deadline" memorandum must be transmitted by the Field Activity Commander to the Director of DLA with a courtesy copy to the General Counsel.
    - ii. This memorandum shall be transmitted through the Under Secretary of Defense for Personnel and Readiness with a carbon copy to the DOD Defense Privacy Office.
10. If the PII does not meet the criteria for being "high impact" and the PII IRT determines it is possible to provide notice to all affected individuals, then the local Counsel's Office will coordinate production of the required notifications and provide them to the affected individuals within 10 business days of discovery of the breach of PII.
11. For non-"high impact" PII incidents, the local Field Activity DLA Office of Investigations point of contact, in consultation with the local Privacy Act Officer and Counsel's Office, will assess the incident to determine if there is a need for an investigation. If such an investigation is necessary, it shall follow standard DLA Office of Investigation/AR-15 procedures applied at the local level. The results of any local incident assessments/investigations will be provided to the local Commander for disposition.
12. If the incident involves "high impact" PII, then the DLA General Counsel's Office, in consultation with the CIO and the field activity involved, will make a determination of whether it will be possible for DLA to provide the required notice to all affected individuals within 10 business days. This notification determination shall be made within 3 business days of discovering the breach of PII.
- a. If the General Counsel determines that it will not be possible to provide notification to the affected individuals within 10 business days, then the General Counsel's office will prepare a memorandum for the Deputy Secretary of Defense for signature by the Director of DLA providing a brief summary of what occurred, why notification was not provided within the required 10 business days, and what actions being taken, highlighting the exact date notifications will commence and their anticipated completion date. Transmit memorandum in accordance with paragraph 9.c.ii. above.
  - b. Otherwise, the General Counsel will prepare the required notifications to the affected individuals with the assistance of the CIO and the field activity involved and provide

that notification within the required 10 business days.

13. For all PII incidents, the DLA General Counsel's Office will provide a report of the incident to the DOD Defense Privacy Office within 48 hours of discovery of the breach of PII.

- a. For non-"high impact" PII incidents, the DLA HQ Privacy Act Officer will forward the report (see 9.a. above) from the Field Activity .
- b. For "high impact" PII incidents, the DLA Chief Privacy Officer will produce and forward the report containing the same elements specified in 9.a. above.

14. In situations involving questions of interpretation, the DLA General Counsel's Office, with DLA CERT providing forensic support, will have final authority in making a determination on whether a breach of personal information/PII has occurred.

15. During the course of a personal information/PII breach investigation, the DLA CERT has the authority to direct tasks be accomplished by each DLA Component, as required, to complete an investigation in a timely manner.

16. Notifications (email or letter<sup>6</sup>) to affected individuals shall contain, at a minimum, the following information:

- a. The individuals shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.
- b. The individuals shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that the individual clearly understands how the compromise occurred.
- c. The individuals shall be informed of what protective actions DLA is taking or the individual can take to mitigate against potential future harm. Steps individuals should take to protect themselves from the risk of identity theft, including the steps identified on the Federal Trade Commission's website, <http://www.ftc.gov/bcp/edu/microsites/idtheft/>. The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.
- d. Contact procedures for those wishing to ask questions or learn additional information, including a telephone number<sup>7</sup>, email address, website, and/or postal address;

17. Incident response reports for data breaches involving PII will be maintained pursuant to DLA Records Retention Schedule, 284.82 Incident (Compromise) Files -- Reports of compromises, involving personnel, cryptologics and physical insecurities of COMSEC material. (Destroy closed incident file after 2 years.) N1-361-91-1

---

<sup>6</sup> Letters are the recommended method for notification involving breaches of personal information/PII from members of the general public.

<sup>7</sup> The point of contact must be someone knowledgeable about the specifics of the breach and understand the steps individuals may take to protect themselves from the risk of identity theft. The Privacy Act Officer or Public Affairs Officer for the field activity where the breach occurs will often be the best suited to handle this activity.